Incident report analysis

Instructions

As you continue through this course, you may use this template to record your findings after completing an activity or to take notes on what you've learned about a specific tool or concept. You can also use this chart as a way to practice applying the NIST framework to different situations you encounter.

Summary	The organization's network services suddenly stopped responding due to an incoming flood of ICMP packets. Normal internal network traffic could not access any network resources. The incident management team responded by blocking incoming ICMP packets, stopping all non-critical network services offline, and restoring critical services. The company's cybersecurity team then investigated the event and found that a malicious actor had sent a flood of ICMP pings into the company's network through an unconfigured firewall.
Identify	Create an inventory of organizational systems, processes, assets, data, people, and capabilities that need to be secured: • Technology/Asset Management: Which hardware devices, operating systems, and software were affected? Trace the flow of the attack through the internal network. • Process/Business environment: Which business processes were affected in the attack? • People: Who needs access to the affected systems? The incident management team audited the systems, devices, and access policies involved in the attack to identify the gaps in security. The team found that a malicious actor had sent a flood of ICMP pings into the company's

	network through an unconfigured firewall.
Protect	Develop and implement safeguards to protect the identified items and ensure delivery of services: • Access control: Who needs access to the affected items? How are non-trusted sources blocked from having access? • Awareness/Training: Who needs to be made aware of this attack and how to prevent it from happening again? • Data security: Is there any affected data that needs to be made more secure? • Information protection and procedures: Do any procedures need to be updated or added to protect data assets? • Maintenance: Do any of the affected hardware, operating systems, or software need to be updated? • Protective technology: Are there any protective technologies, like a firewall or an intrusion prevention system (IPS), that should be implemented to protect against future attacks?
Detect	Design and implement a system with tools needed for detecting threats and attacks: • Anomalies and events: What tools could be used to detect and alert IT security staff of anomalies and security events, such as a security information and event management system (SIEM) tool? • Security continuous monitoring: What tools or IT processes are needed to monitor the network for security events? • Detection process: What tools are needed to detect security events, such as an IDS?

Respond	Design action plans for responding to threats and attacks: • Response planning: What action plans need to be implemented to respond to similar attacks in the future? • Communications: How will security event response procedures be communicated within the organization and with those directly affected by the attack, including end users and IT staff? • Analysis: What analysis steps should be followed in response to a similar attack? • Mitigation: What responding steps could be used to mitigate the impact of an attack, such as offlining or isolating affected resources? • Improvements: What improvements are needed to improve response procedures in the future?
Recover	Construct a plan and implement the framework for recovering and restoring affected systems and/or data: • Recovery planning: How will resources be restored following an attack? • Improvements: Do any improvements need to be made to the current recovery systems or processes? • Communications: How will restoration procedures be communicated within the organization and with those directly affected by the attack, including end users and IT staff?

Reflections/Notes: